Computer Forensics as an Integral Component of the Information Security Enterprise

By John Patzakis

215 North Marengo Avenue, Second Floor • Pasadena, California 91101 • Tel. 626.229.9191 • www.guidancesoftware.com

I. EXECUTIVE SUMMARY

In addition to fending off network intrusions and denial of service attacks, companies must also contend with many other threats to their information infrastructure and assets. Industrial espionage, employee misconduct, and intellectual property theft are among the computer security incidents that increasingly plague corporate organizations. The American Society of Industrial Security and the FBI report the theft of intellectual property in the United States costs businesses approximately $24 billion annually.[1] Additionally, the vast majority of information in the workplace is now stored on PCs and servers, meaning that no internal investigation of any form should ignore digital evidence.

Computer incident response procedures must include proper computer forensics protocol to properly secure, recover, and authenticate relevant computer evidence in order to facilitate its admission into a court of law. The proper collection and analysis of computer evidence with computer forensics software is critical in criminal investigations, civil litigation matters, and corporate internal investigations. Finding the "smoking gun" will likely not benefit an investigation if the examiner cannot establish that the subject data was not corrupted or tampered with.

This paper provides an overview of computer forensics and addresses recent developments as well as future trends impacting the field. Specific topics examined include how computer forensics is making an important transition from a "black art" relegated to a select few experts to a requisite component of the information security enterprise, and how new technology is enabling computer forensics to evolve into a broader process, incorporating proactive computer investigations and information systems auditing.

II. INTRODUCTION

Computer forensics is commonly defined as the collection, preservation, analysis, and court presentation of computer-related evidence. Courts mandate the proper seizure and analysis of computer evidence in any investigation where a computer is the means or an instrument of a crime or other offense or may contain evidence relevant to a criminal or civil litigation matter.[2] The rising tide of computer-related intellectual property theft, security breaches, and associated financial losses mandates that information security administrators conduct or oversee proper computer forensic investigations when responding to these incidents.

The most important tool for a computer forensic investigator is the software used to perform the investigation. Without specially designed computer forensic software, there cannot be a true forensic analysis. In general, there are three primary reasons why specialized computer forensic software must be employed in order to conduct a proper computer investigation:

1. Proper Acquisition and Preservation Of Computer Evidence

Electronic evidence is fragile by nature and easily can be altered or erased without proper handing. Merely booting a subject computer into a Windows environment will alter critical date stamps, erase temporary data, and cause hundreds of writes to the drive. Specialized computer forensic software, such as EnCase, ensures the subject computer's data is not altered in any way during the acquisition process. After initiation of the special boot procedure, the examiner utilizes computer forensic software to create a bit-stream image, or an "exact snapshot," of the subject hard drive and all other external media, such as floppy or zip disks, which are subject to the investigation. The evidentiary image must be a complete, non-invasive, sector-by-sector copy of all data contained on the target media in order to recover all active, deleted, and otherwise unallocated data, including often critical file slack, clipboards, printer spooler information, swap files, and data contained or hidden in bad sectors or clusters. The process allows the investigator to freeze time by having a complete snapshot of the subject drive at the time of acquisition.

After the image copy is created, computer forensic software will mount the image as a read-only drive, thus allowing the investigator to conduct the examination on the image of the subject drive without altering the contents of the original. This process is essentially the only practical means to search and analyze computer files without altering date stamps or other information. Often, a file date stamp is a critical piece of evidence in litigation matters.

2. Authentication of Collected Data for Court Presentation

Computer forensics is based largely on the premise that the data recovered from computer systems will ultimately be presented in a court of law. As such, another important feature of computer forensic software is a verification process that establishes that the investigator did not corrupt or tamper with the subject evidence at any time in the course of the investigation.

Computer forensic software employs a standard algorithm to generate an image hash value. The algorithm calculates a unique numerical value based upon the exact contents contained in the evidentiary image copy. If one bit of data on the acquired evidentiary bit-stream image changes, even by adding a single space of text or changing the case of a single character, this value changes.

The most common hashing process utilized is the MD5 (Message Digest number 5), which is based on a publicly available algorithm developed by RSA Security. The odds of two computer files or two images of drives with different contents having the same MD5 hash value is roughly ten raised to the 38th power, or one followed by 38 zeros (One trillion is one followed by just twelve zeros.) The MD5 hash function allows the examiner to confidently stand by the integrity of the data in court.

An IS administrator should approach every computer investigation with the assumption that the image of the targeted computers will ultimately be turned over to company lawyers or law enforcement for civil litigation or criminal prosecution purposes. The creation of an evidentiary image copy that is verified and authenticated pursuant to proper computer forensic protocol is essential to ensure a smooth transition from the response stage of the investigation to the enforcement or litigation process.

3. Recovery of all Available Data, Including Deleted files

In addition to the active data normally seen by the computer user, computer forensic software allows the examiner to recover all deleted files that have not been completely overwritten, as well as other forms of unallocated or temporary data. Information contained in swap files, printer spooler files, file slack, and other temporary or buffer files are examples of data residing on a computer drive that are not normally visible to the user. As noted previously, this information must be recovered non-invasively.

Additionally, successful computer forensic investigations often depend on advanced techniques, such as recovering temporary files from unallocated clusters or locating and decoding Windows artifacts such as recycle bin info. files, deleted registry entries, metafiles, and log files. Advanced computer forensic tools are designed to efficiently extract this information, allowing the investigator to conduct a complete and thorough investigation. Perhaps more importantly, advanced computer forensic software will identify and document the exact location on the original drive from which the investigator recovered such transient data.

III. A NEW MODEL FOR COMPUTER FORENSICS

The latest generation of Windows platform tools led by EnCase by Guidance Software has redefined the field of computer forensics by providing a dramatically more efficient process. Prior to the recent development of integrated GUI-based tools, forensic investigators toiled with various procedures that required numerous non-integrated DOS or Unix-based utilities in a process that was inefficient, costly, burdensome, and often incomplete and inaccurate. Under the old methodology, examiners often spent weeks examining a small two GB hard drive and still missed critical pieces of evidence. Further, few could conduct investigations as command-line analysis required extensive expertise in the DOS or Unix file system and the mastery of hundreds of arcane commands and switches.

Viewed by many CIOs and other IS managers as impractical and costly, market forces relegated the practice of computer forensics in the private sector to a relatively small group of consultants. This early community of consultants perpetuated the perception of computer forensics as a “black art,” urging companies and law firms to leave the practice to the experts. In fact, before the availability of EnCase and thus the simplification of the computer forensic process, one industry expert suggested that companies consider not bothering with the process, noting, “When people hear about computer forensics, they think it sounds like fun…. In fact, it is a lot of work.”[3] So much work, in fact, that any benefit gained from a proper forensic investigation often could not justify the extensive time and resources spent in the process.

The early pioneers of computer forensics also believed that forensic examinations should never take place in a Windows environment as Windows routinely alters data and writes to the hard drive. However, the latest generation of computer software tools resolves this problem by non-invasively acquiring the evidence and then mounting the resulting bit-stream image as a read-only drive. The forensic software, not the operating system, then reconstructs the file system of the acquired drive by reading the logical data on the image backup, thus allowing the examiner to view, sort and analyze the data through a Windows graphic user interface in a completely non-invasive manner.

Additionally, all of the necessary tools and functions are now integrated into one application, further streamlining the investigation process and allowing the examiner to multitask, manage the evidence more effectively, and build a case. The new generation of forensic software is expanding the practice of computer forensics by providing a powerful yet highly efficient solution that allows for comprehensive and dramatically more cost-effective investigations by reasonably skilled IS professionals.

IV. BEYOND INCIDENT RESPONSE

Computer investigations in some form routinely take place at any typical Fortune 1000 company. As such, it is incumbent upon IS managers to ensure that their security personnel and auditors employ proper computer forensics tools and techniques in the course of these investigations. Fortunately, with the advent of a new generation of computer forensic software, the implementation of proper forensic investigation practice and protocol is both technically feasible and cost efficient.

With the supporting technology becoming increasingly powerful and efficient, coupled with increased emphasis on information assurance and security, computer forensics is quickly becoming standard protocol in corporate internal investigations by expanding beyond the realm of specialized computer incident response teams. As the overwhelming majority of documents are now stored electronically, it is difficult to imagine any type of investigation that does not warrant a computer forensic investigation.

Computer forensics software now features advanced analysis functions, providing the ability to accurately search, analyze, and manage large volumes of computer data. Among such capabilities is the ability to conduct examinations over a local or even a wide area network. Computer forensics is therefore transitioning from merely an investigation and response mechanism to a powerful proactive measure. In addition to computer incident response personnel, IT auditors are increasingly employing computer forensics software to quickly detect non-compliant software, improper computer usage, and system vulnerabilities.

Additionally, many corporate legal counsels are working with the IT staff and auditors to implement policies that take advantage of new computer forensics capabilities. At one Fortune 500 company, for instance, an employee's hard drive is imaged upon resignation, termination, or internal transfer as a matter of standard procedure. The images are then archived to CD-ROM disks should an examination need to take place at a later date. Preserving and archiving these images is important, as issues such as theft of trade secrets or intellectual property, harassment, and wrongful termination claims often do not surface until months after an employee leaves his or her position, at which point the critical computer evidence has been overwritten.

Computer forensics software is also utilized to search across networks and servers for information in response to litigation discovery or pursuant to records management and document retention policies. The ability to efficiently and effectively manage and analyze large volumes of computer data is clearly a new prerequisite for computer forensic software.

V. CONCLUSION

With organizations incurring far too excessive losses of intellectual property and other trade secrets, advancements in computer forensics technology are meeting the compelling need to counter this threat. With this improved technology and infrastructure, ongoing and proactive computer investigations are now a mandatory component of the information security enterprise.

NOTES

[1] http://www.fbi.gov/hq/cid/fc/fifu/about/about_ipc.htm
[2] *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*, 167 F.R.D. 90 (D.C. Col., 1996) is a particularly important published court decision in this area, in which the court ruled that when processing evidence for judicial purposes a party has "a duty to utilize the method which would yield the most complete and accurate results."
[3] "Computer Forensics" SC Magazine (1998), Vol 9, no 10 (available online at http://www.scmagazine.com/scmagazine/1998_10/cover/cover.html)